1. PURPOSE

The purpose of this document is to establish an understanding that the user has the primary responsibility to safeguard the Information Systems (ISs) managed by the Enterprise Information Technology Project Management Office (eIT PMO). The eIT PMO manages a suite of IT capabilities connected to the Unclassified but Sensitive Nonsecure Internet Protocol Router Network (NIPRNET) to include the Electronic Document Management System (EDMS), Serious Adverse Event (SAE), the Electronic Data Capture (EDC), and the Electronic Common Technical Document (eCTD) products. Army Regulation (AR) 25-2 mandates the requirement for an Acceptable Use Policy (AUP) detailing the responsibilities of each Government Information System (IS) user. Federal Government information and communication systems include but are not limited to: government owned hardware (e.g. computers, telephones, printers, facsimile machines, scanners); government software applications (e.g. office automation, electronic e-mail); Intranet and Internet; and commercial systems when use is paid for by the Federal Government. All users of the eIT PMO's products must read this AUP and sign the Acknowledgement stating that they have read, understand, and accept their responsibilities regarding use of the eIT's suite of IT products as well as the information stored within the products.

2. REFERENCES AND RELATED DOCUMENTS

- AR 25-2, Information Assurance
- AR 25-4-14, Personnel and Access Security Requirements
- AR 25-55, Information Assurance, Section 4-200
- AR 380-53, Information Systems Security Monitoring
- Application Security and Development Checklist
- DODI 8500.2, Information Assurance (IA) Implementation
- DODI 8500.3, Identity Authentication for Information Systems (ISs)
- USAMRMC Local Memorandum 25-2-1
- 04-IA-O-0001 Army Password Standards v 2.5
- Web Application Security Technical Implementation Guide (STIG) 3320 v 6130

3. POINTS OF CONTACT

Questions regarding this document may be directed to the USAMITC Enterprise Service Desk at :
web: https://esd.amedd.army.mil; or phone: 1-800-872-6482
or email the eIT PMO at usarmy.detrick.medcom-usamrmc.other.eit-pmo@mail.mil.

4. MINIMUM SECURITY RULES AND REQUIREMENTS

As a Government Information System (IS) user, the following minimum security rules and requirements apply:

a. The acceptable requirements for accessing eIT PMO Information Systems include:

(1) Generating, storing, and protecting passwords when required for access to applications. Passwords will consist of 14 characters (per Web STIG) with 2 each of uppercase and lowercase letters, numbers, and special characters. Password shall be changed every 60 days and will not use

any of the previous 10 passwords, user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words. Account(s) shall not be shared.

(2) Using virus-checking procedures before uploading or accessing information from any system, attachment, diskette, compact disk (CD), digital videodisk (DVD), or removable storage device.

(3) Not attempting to process or store classified data within the eIT's suite of IT products.

(4) Not introducing executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor writing malicious code.

(5) Decide, from a business perspective, whether to store **For Official Use Only (FOUO)** in the system, and if so, acknowledge FOUO data in the system.

- It is appropriate to access FOUO data only over an approved VPN connection. Do not access eIT Information Systems via a public computer, i.e., library, hotel lobby.
- Safeguarding and marking the appropriate classification level on all information created, copied, stored, or disseminated from eIT Information Systems, i.e., FOUO.
- **NOTE**: Non-DoD collaborators have account access on some of the eIT Information Systems. Be careful in posting FOUO information, as non-DoD collaborators should not be viewing FOUO documents unless granted access by their Government Sponsor. Do not disseminate FOUO documents to anyone without a specific need to know, in order to prevent unauthorized public disclosure.
- Regulations require printing of documents that contain FOUO information be marked with a **For Official Use Only** label at the top and bottom of each page when non-DoD collaborators have access.

(6) Using screen locks when away from the workstation, even for a brief time. If the workstation is not in line of sight, log off workstation when departing the area.

(7) Immediately reporting any suspicious output, files, shortcuts, or system problems to the Enterprise Service Desk at 800USAMITC@amedd.army.mil and ceasing all activities on the system.

(8) Understanding that monitoring of the eIT IS will be conducted for various purposes and information captured during monitoring may be used for administrative, disciplinary actions, or for criminal prosecution.

(9) Understanding that any activity that occurs using my account is my responsibility.

(10) Understanding that storage or transmission of personal medical data or Privacy Act material is prohibited within the eIT's suite of IT products.

b. Unacceptable use of the eIT ISs includes, but is not limited to:

(1) Introducing malicious code or conducting other hacking like behavior on an eIT IS.

(2) Using the system to store personal files that are not used to conduct business, such a photos, videos, and/or music files.

(3) Conducting a commercial business on an eIT IS.

(4) Unethical uses (e.g. profanity, sexual content, gambling, soliciting funds).

(5) Sharing of passwords and accounts.

(6) Attempting to access or transmit data exceeding the authorized IS classification level, (eIT's level is unclassified, sensitive).

(7) Storage of Personally Identifiable Information (PII) or Personal Health Information (PHI).

5. ENFORCEMENT

All users that do not comply with this document will have their access suspended and possibly deleted from any and all eIT ISs.

6. ACKNOWLEDGEMENT

By signing this document, you acknowledge and consent to the following conditions when accessing eIT's ISs:

a. The U.S. Government routinely intercepts and monitors communications on eIT ISs for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct, law enforcement (LE), and counterintelligence (CI) investigations.

b. Communications using, or data stored on, the eIT ISs are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

c. eIT ISs includes security measures (e.g. authentication and access controls) to protect U.S. Government interests, not for personal benefit or privacy.

d. Notwithstanding the above, using eIT ISs does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work products are private and confidential, as further explained below:

- Nothing in this document shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government action for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personal misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personal misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy.
- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

e. In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise authorized use or disclosure of such information.

f. All of the above conditions apply regardless of whether the access or use of an IS includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this document, regardless of whether the banner describes these conditions in full detail, or provides a summary of such conditions, and regardless of whether the banner expressly references this document.

7. ACCOUNT APPROVALS INSTRUCTIONS:

- **FILL OUT AND SIGN "REQUESTOR" SECTION.**
- NON DoD MUST OBTAIN SIGNATURE OF **GOV'T SPONSOR. (GOV'T SUPERVISOR OF THE BRANCH/ DIVISION SPONSORING THE EXTERNAL COLLABORATOR, OR HAS CONTRACT/AGREEMENT OVERSIGHT; GRADE 04 OR ABOVE, OR GS-13 OR ABOVE).**
- **ATTACH AUP SIGNATURE PAGE AND DoD IA TRAINING CERTIFICATE TO ACCOUNT REQUEST FORM MRMC 25-2; FORWARD TO usarmy.detrick.medcom-usamrmc.other.eit-pmo@mail.mil .**
- **QUESTIONS, CONTACT eIT PMO AT THE ABOVE EMAIL ADDRESS.**

REQUESTOR: I have read the above requirements regarding use of eIT Information Systems. I understand all terms and conditions in this Acceptable Use Policy (AUP) and accept my responsibilities and accountability regarding these systems and the information contained in them.

_____ _____

Date: **Requestor Last Name, First, MI *(Print)***

_____

Name of Business / Organization

_____ _____

Requestor Email Address **Requestor Phone Number**

Signature or Electronic Signature of User Requesting an Account **X** _____

ENDORSEMENT FOR ACCESS (NEED TO KNOW) BY GOVERNMENT SPONSOR FOR THE ORGANIZATION SPONSORING EXTERNAL COLLABORATOR

I am verifying that the aforementioned Requestor requires access as requested.

_____ _____

Date: **Government Sponsor Last Name, First, MI *(Print)***

_____ _____

Government Sponsor Email Address **Phone Number**

Government Sponsor Signature or Electronic Signature Endorsing Requestor's "Need to Know" **X** _____